BCA/Border Directory Issues

Bill Burr
National Institute of Standards and Technology
301-975-2914
william.burr@nist.gov
February 11, 1999

Directory Products

- Roughly 3 kinds of products:
  - X.500 DSA
    - » DSP chaining
  - LDAP server
    - » no DSP, often tied to specific app. or OS
  - Meta-Directory
    - » ties different kinds of products together
      - DSP, LDAP & others

X.500 DSA

- DAP and LDAP access
- DSP
  - interproduct chaining (often) works
  - replication features more problematic
- Moderately mature products
- Not tied to specific app. products
- Perceived as expensive
  - specialized care & feeding

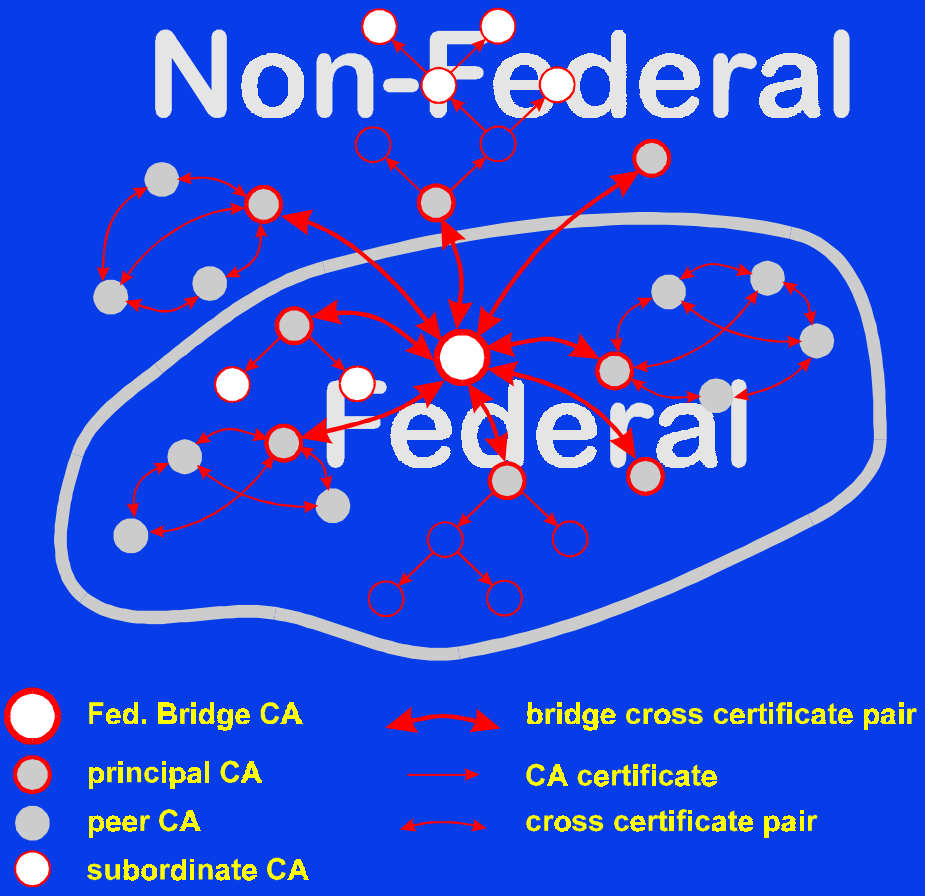
LDAP Server

- LDAP client access
  - LDAP v2 & v3 (only v3 does referrals)
- No DAP or DSP
  - proprietary chaining, replication
    - » LDAP standards someday?
- Often tight OS or application linkage
  - some with big market share
    - » care & feeding lumped with application
    - » often coupled with CA product

Meta-Directory

- New product category
- Ties together different directories
  - LDAP server, X.500 & e-mail, etc.
  - integrates one "virtual" view of all
- Cost and complexity??
  - care and feeding issues
    - » hard to set up basic directory products
    - » may be a consultant's dream come true
- Performance??

Bridge CA PKI Architecture



First BCA Directory Proposal

- One stop CA certificate shopping
  - CA certs. for the Federal PKI
  - ARL
- Didn't discuss BCA directory chaining/ referrals, etc.
  - How are end entity certificate made available?

Border Directory Proposal

- Each agency has a Border Directory
  - for publicly available EE certs & CRLs
    - » may shadow part of local directory system
    - » CAs may publish directly in border directory
    - » unrestricted read access
  - outside agency firewall
  - chain (X.509 DSP) to BCA DSA
    - » requires “proper X.500” DSA

Border Directory Proposal

- Connection of border directory to internal agency directory not defined
  - alternatives:
    - » chaining
    - » shadowing
    - » direct publication by CAs into border directory

Border Directory Proposal

- User Access to FPKI BCA directory
  - agency option
  - probably an extension of internal directory access
    - » Internal X.500 DSAs probably chain to border directory or BCA directory
    - » Others internal directory servers may refer clients to border directory or BCA directory

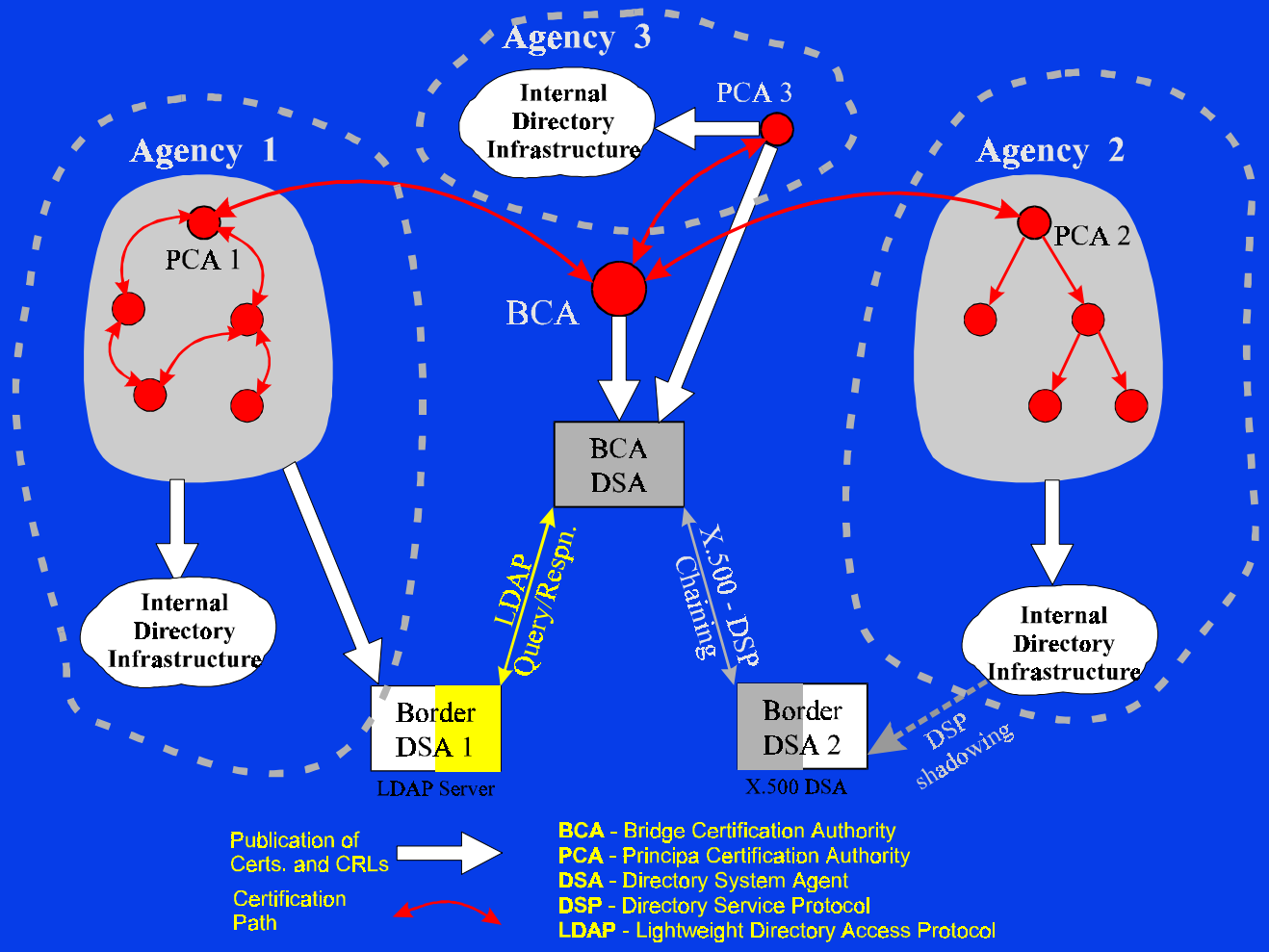
Border Directory Problems

- Agencies must stand up X.500 DSA
  - some agencies have no X.500 directories
    - » LDAP servers, proprietary, or nothing
      - LDAP servers tied to OS or major apps
  - care and feeding issues
    - » X.500 DSAs complex products
    - » chaining directories can be challenging
  - X.500 DSAs seen as expensive

Expanding the Concept

- BCA directory is PKI directory nexus
  - Link to X.500 border DSAs via DAP chaining, but
  - Link to LDAP oriented agencies without forcing them to stand up an X.500 DSA
- External directory hosting service
  - GSA & US Gold?
  - NTIS in BCA directory itself?
  - other agencies border directory?
  - commercial directory hosting service?

Expanded BCA Directory



“Publication” to Directory

- Local option to agency internal or border directory,
  - DAP, LDAP, floppy disk, passenger pigeon, etc.
- External host directory (including BCA) will need specified mechanisms

Expanded BCA Directory

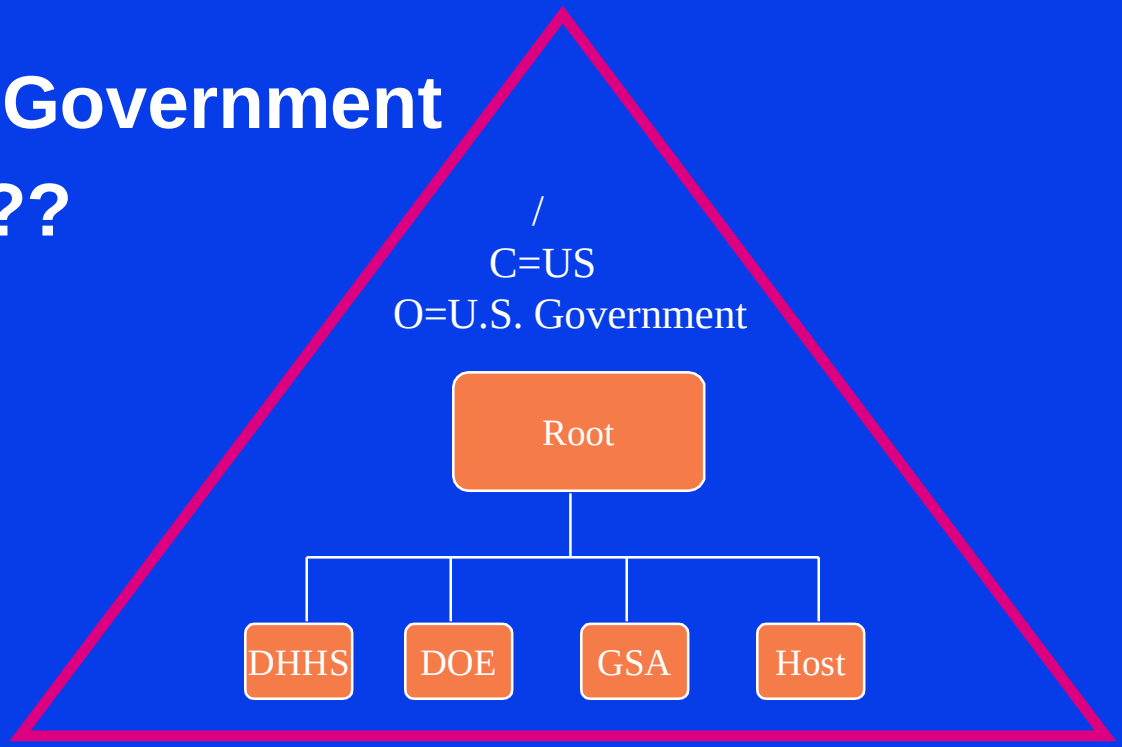
- **BCA directory needs to connect to LDAP servers as well as X.500 DSAs**
  - **convert DSP queries to LDAP**
    - » **apparently some products can do this**
    - » **need a full-blown Meta-Directory product?**
      - lets keep things as simple as we can
      - we're not about a comprehensive Federal Gov. Meta-Directory
        - but US Gold might evolve to that

PKIX LDAP v2 Schema

- Schema for PKI object classes
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-ldapv2-schema-02.txt
  - may not be implemented yet in some products
  - is there another game in town?

US Government DIT

- GSA is naming registration authority
  - C=US
  - O=U.S. Government
  - OU=????



US Gold Role?

- Now (with Directory Forum) focused on e-mail & telephone listings for Gov. employees.
- A hosting service for agencies that don't want their own border directory?
- Should it be the BCA directory?

Approach

- Start simple
  - lots of problems to solve
- X.500 DSP chaining easiest thing to do first
  - Add border directory hosting
  - Add LDAP “bridge” as soon as we can
- grow directory as we grow PKI

Conclusion

- Access both end-entity & CA certs.
- Agencies will want border directories
- Directory equivelent of BCA to link several types of border directories
  - X.500 DSA
  - LDAP server
- Start simple and evolve